MIMOTEC GigaLink AC

User Manual

Version 1.5 (8 January 2014)

General

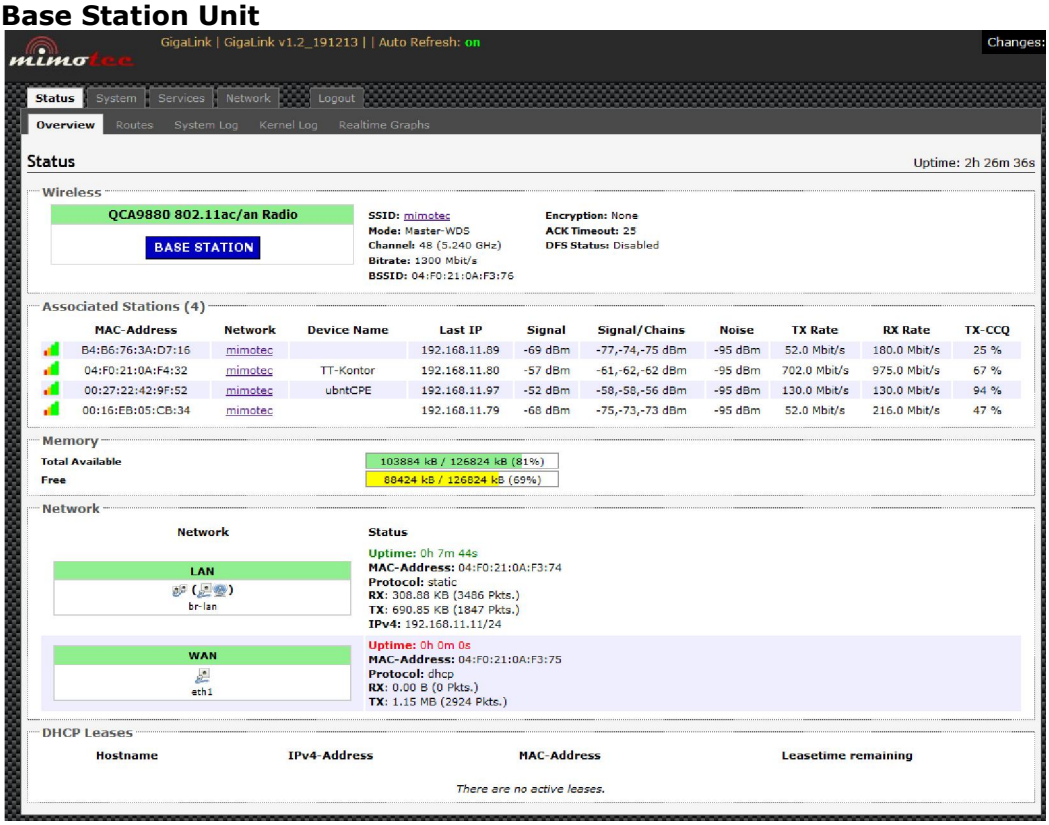
MIMOTEC GigaLink AC is a family of high capacity point to point and point to multipoint system for access networks and backhauling applications. The user interface on GigaLink is based on OpenWRT (Luci) and is structured with focus on simplicity and speed, and does not provide much selectable and advanced options, as the most favorable settings is applied automatically. This allows operators to setup high capacity systems with less effort and expertise than comparable alternatives.

All wireless connections for GigaLink operates fully adaptive, and will provide Link Rate depending on channel bandwidth settings, link quality and capacity needed. This provides a more flexible application than traditional Micro Wave systems, when GigaLink is used for PtP backhauls.

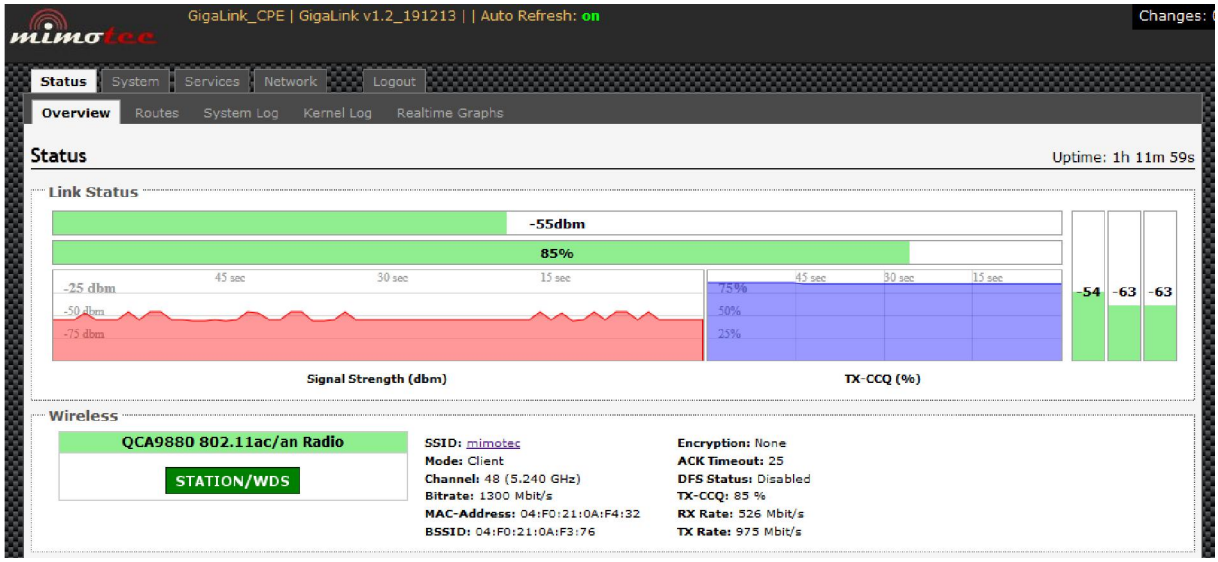
GigaLink system administration is mainly done via WEB-browser, but may also be managed trough CLI (Linux shell) via SSH. Use an up to date WEB-browser (Chrome, Firefox or Opera recommended).

GigaLink Default settings:
IP-address 192.168.1.1/24 – Username: *admin* – Password: *default*
Enter username and password:

The WEB start page – Status Menu:
Base Station Unit



CPE Unit



The Status window is read-only information, and will give the user an instant overview of on unit status. The info-bar at the top shows the running Firmware version.

The Menu structure:

<u>Status</u>

- Overview: — Gives an instant overview on unit status and connections
- Routes — Shows IP sub-net configurations and gateways
- System Log — Shows system log for kernel, deamon and user level
- Kernel Log — Shows kernel and driver logs
- Realtime Graphs
  - Load — Shows average and peak CPU load for last 3 minutes
  - Traffic — Shows average and peak traffic load for last 3 minutes
  - Wireless — Shows average and peak signal levels and noise for last 3 minutes
  - Connections — Shows average and peak connection numbers for last 3 minutes

<u>System</u>

- System — General settings for hostname, timeserver and syslog
- Administration — Admin password setting and SSH configuration
- Services — Settings for ping-watchdog and auto-reboot
- SNMP — SNMP administration for read/write community
- LED Configuration — For adjusting the LED/GUI-color for signal thresholds
- Backup/Flash — For unit backup/restore and flashing new firmware.
- Reboot — For rebooting the unit

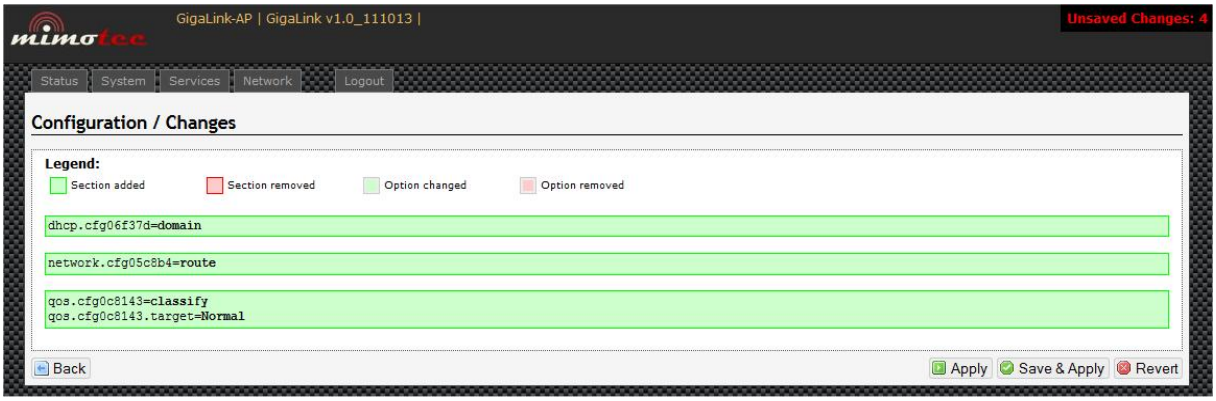
<u>Services</u> — For configuring Dynamic DNS settings

<u>Network</u>

- Interfaces — Shows status and configuration of LAN/WAN interfaces
- WiFi — Shows status and configuration of wireless configuration
- Hostnames — For manually adding hostnames and corresponding IP
- Static Routes — For manually setting static routes and gateways
- Firewall
  - General Settings — For defining firewall rules and zones
  - Port forwards — For adding port forward rules and DMZ
  - Traffic Rules — For controlling interface packet flow and source NAT
- Diagnostics — For controlling ping, traceroute and NS-lookup
- QoS — For setting CIR/MIR and service/protocol limitations

Saving changes in the menus

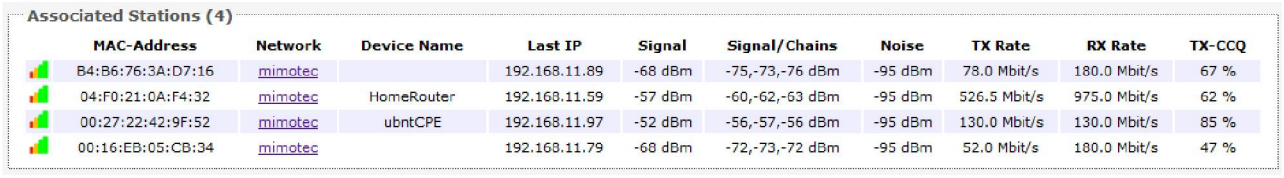
After changes made from each respective menus, the unsaved changes will be indicated at the top status field:



User may Save and Apply all changes in one operation - or revert all changes. A list of all configuration settings will be listed if user click on the "Unsaved Changes" in the status field at the top. The unit will not require a reboot, it will just do a reload of configuration when Save and Apply is selected.

Base Station - Status information

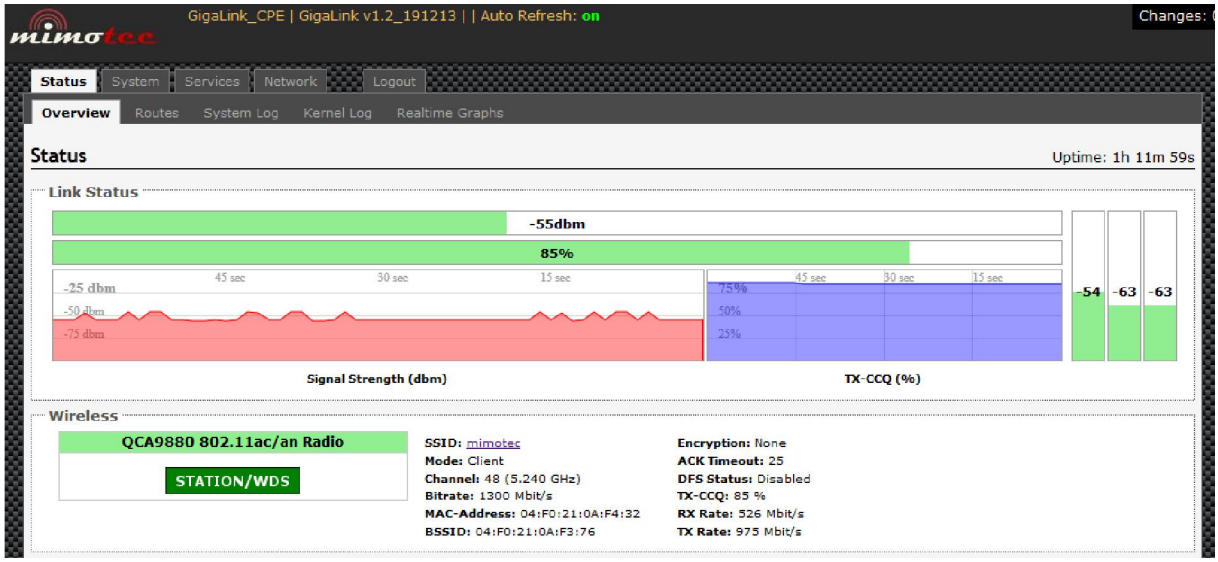
If configured as Base Station, the Status Overview menu will show the status and configuration of the wireless interfaces and details on the connected Stations:



- The color-bars indicating the Rx signals from connected stations (controlled by the LED threshold settings under System/LED settings):
- MAC address of the connected stations
- What SSID the stations are associated with
- Device Name as broadcasted by discovery (Mikrotik and UBNT compatible)
- Rx signal from the stations, pr Chain, in dBm
- Detected Noise Level at the interface
- Rx and Tx rates (Link Rates for corresponding MCS)
- Tx CCQ - Transmit Client Connection Quality as a factor of % successfully transmitted RF frames

Station/CPE - Status information

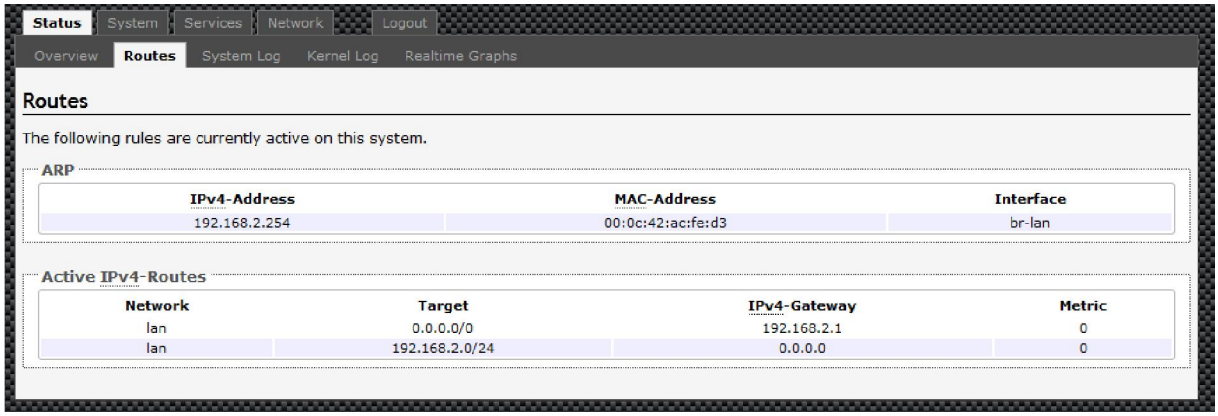
If configured as Station/CPE, the Status Overview menu will show the status and configuration of the wireless interfaces:



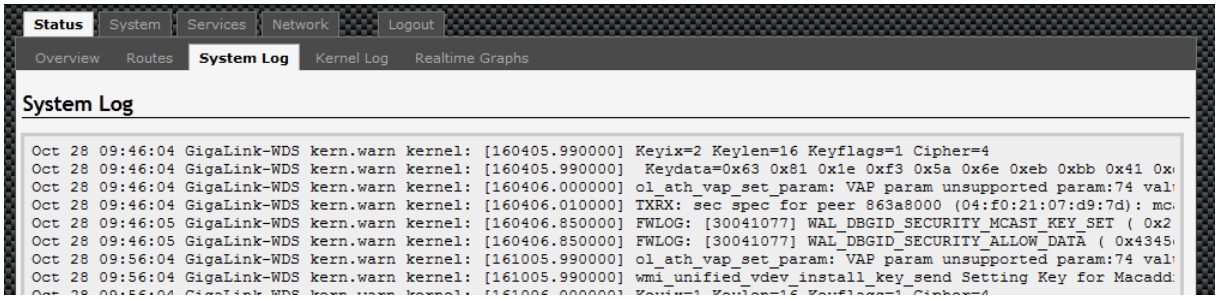
- Link Status showing the overall received signal level
- Graph of last minute of Rx signal level for convenient alignment help
- Last minute graphs for Tx-CCQ for indication of connection quality in % of successfully transmitted RF-frames
- Way to the right are the bars for indicating the Rx levels pr MIMO chains. The 3rd chain for 2x2 MIMO will show a positive value, but not be valid.

STATUS – menus

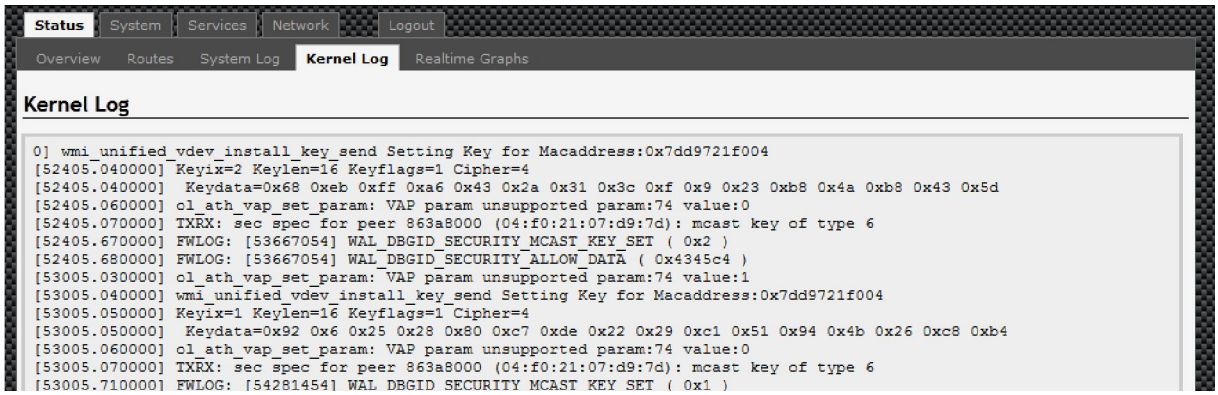
Routes, this menu shows the running routing configurations and ARP entries:



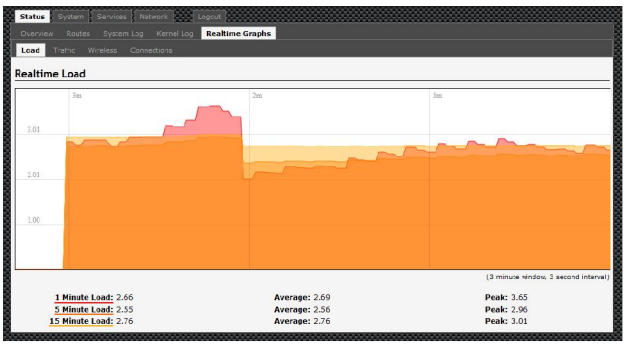
System Log, This menues shows logs from the ystem and kernel:

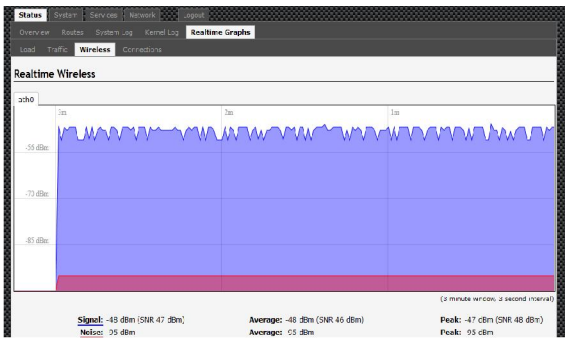

Status
System
Services
Network
Logout
Overview
Routes
System Log
Kernel Log
Realtime Graphs
System Log
Oct 28 09:46:04 GigaLink-WDS kern.warn kernel: [160405.990000] Keyix=2 Keylen=16 Keyflags=1 Cipher=4
Oct 28 09:46:04 GigaLink-WDS kern.warn kernel: [160405.990000] Keydata=0x63 0x81 0x1e 0xf3 0x5a 0x6e 0xeb 0xbb 0x41
Oct 28 09:46:04 GigaLink-WDS kern.warn kernel: [160406.000000] ol_ath_vap_set_param: VAP param unsupported param:74
Oct 28 09:46:04 GigaLink-WDS kern.warn kernel: [160406.010000] TXRX: sec spec for peer 863a8000 (04:f0:21:07:d9:7d):
Oct 28 09:46:05 GigaLink-WDS kern.warn kernel: [160406.850000] FWLOG: [30041077] WAL_DBGID_SECURITY_MCAST_KEY_SET (0x2
Oct 28 09:46:05 GigaLink-WDS kern.warn kernel: [160406.850000] FWLOG: [30041077] WAL_DBGID_SECURITY_ALLOW_DATA (0x4345
Oct 28 09:56:04 GigaLink-WDS kern.warn kernel: [161005.990000] ol_ath_vap_set_param: VAP param unsupported param:74
Oct 28 09:56:04 GigaLink-WDS kern.warn kernel: [161005.990000] wmi_unified_vdev_install_key_send Setting Key for Macadd

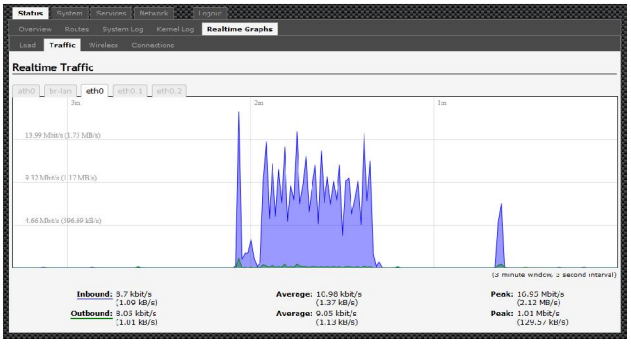
Kernel Log, this menu shows messages created by the kernel:

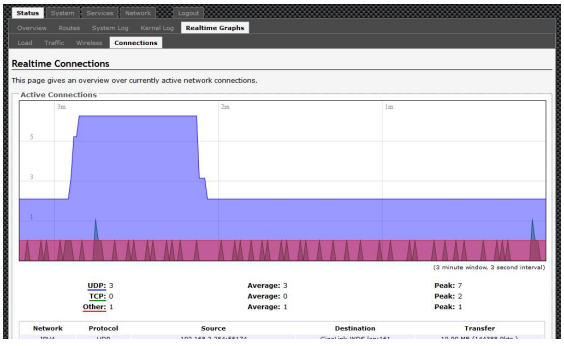

Status
System
Services
Network
Logout
Overview
Routes
System Log
Kernel Log
Realtime Graphs
Kernel Log
0] wmi_unified_vdev_install_key_send Setting Key for Macaddress:0x7dd9721f004
[52405.040000] Keyix=2 Keylen=16 Keyflags=1 Cipher=4
[52405.040000] Keydata=0x68 0xeb 0xff 0xa6 0x43 0x2a 0x31 0x3c 0xf 0x9 0x23 0xb8 0x4a 0xb8 0x43 0x5d
[52405.060000] ol_ath_vap_set_param: VAP param unsupported param:74 value:0
[52405.070000] TXRX: sec spec for peer 863a8000 (04:f0:21:07:d9:7d): mcast key of type 6
[52405.670000] FWLOG: [53667054] WAL_DBGID_SECURITY_MCAST_KEY_SET (0x2)
[52405.680000] FWLOG: [53667054] WAL_DBGID_SECURITY_ALLOW_DATA (0x4345c4)
[53005.030000] ol_ath_vap_set_param: VAP param unsupported param:74 value:1
[53005.040000] wmi_unified_vdev_install_key_send Setting Key for Macaddress:0x7dd9721f004
[53005.050000] Keyix=1 Keylen=16 Keyflags=1 Cipher=4
[53005.050000] Keydata=0x92 0x6 0x25 0x28 0x80 0xc7 0xde 0x22 0x29 0xc1 0x51 0x94 0x4b 0x26 0xc8 0xb4
[53005.060000] ol_ath_vap_set_param: VAP param unsupported param:74 value:0
[53005.070000] TXRX: sec spec for peer 863a8000 (04:f0:21:07:d9:7d): mcast key of type 6
[53005.710000] FWLOG: [54281454] WAL_DBGID_SECURITY_MCAST_KEY_SET (0x1)

Realtime Graphs, this menu shows graphs for System Load, Traffic, Wireless and connections - given for the last 3 minutes:



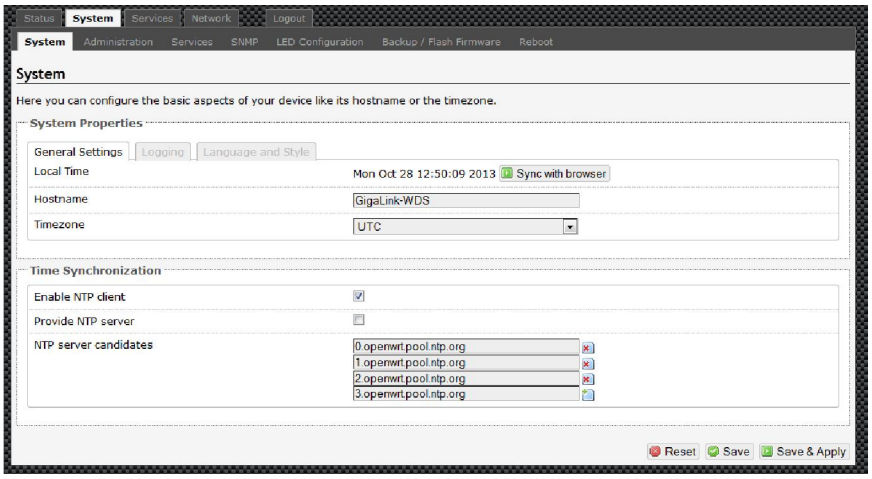




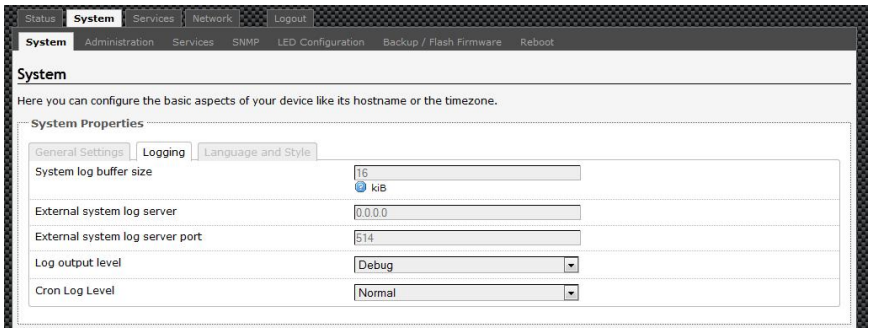


SYSTEM – menus

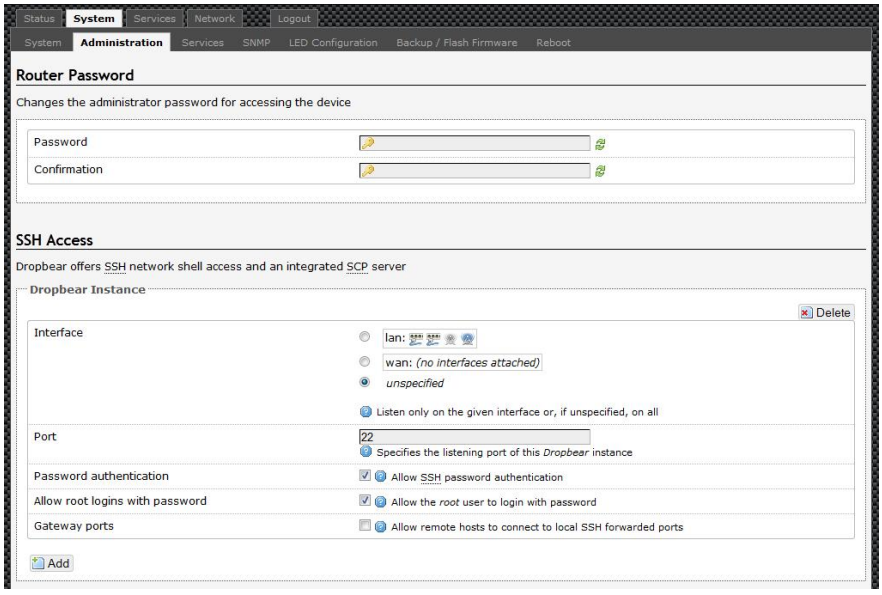
System - System menu, allows the user to input Hostname and NTP parameters and Time Zone.



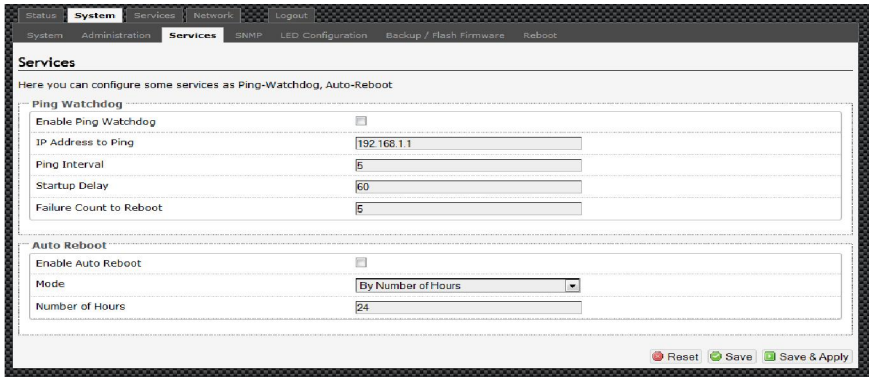
System Logging, for remote Syslog Service



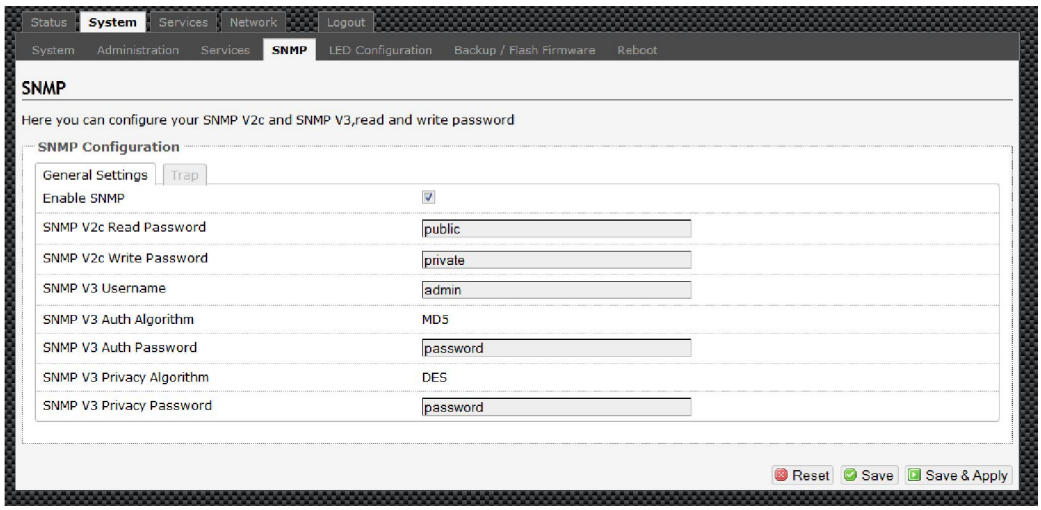
System - Administration, for setting/changing admin passwords, and specifying SSH access parameters:

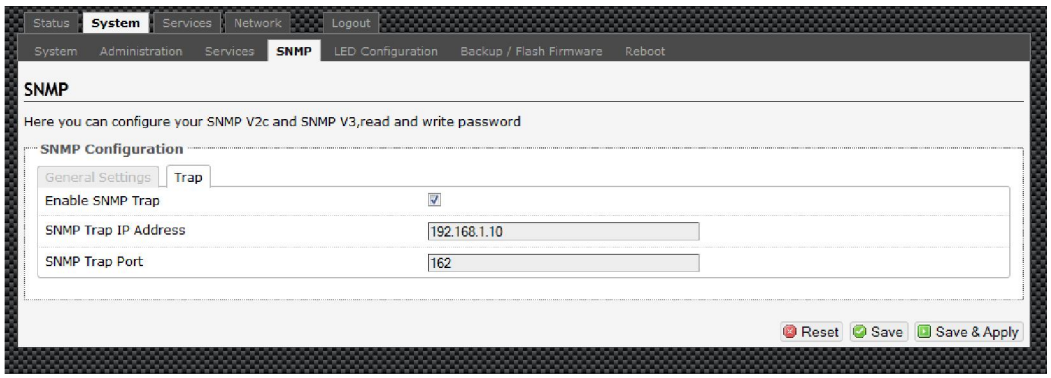


System - Services, allows user to set a Ping Watchdog configuration and specify a Auto Reboot setting:

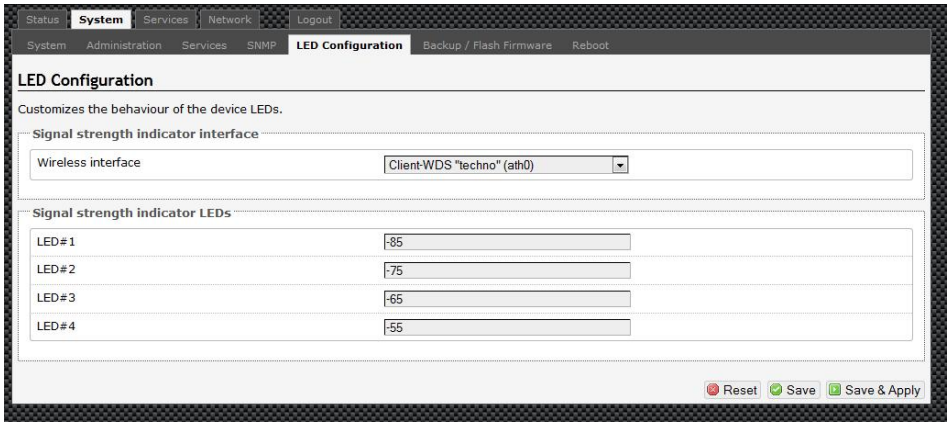


System - SNMP, allows user to specify SNMP service (supports v1, v2, and v3 - read and write), and specify a SNMP Trap host:

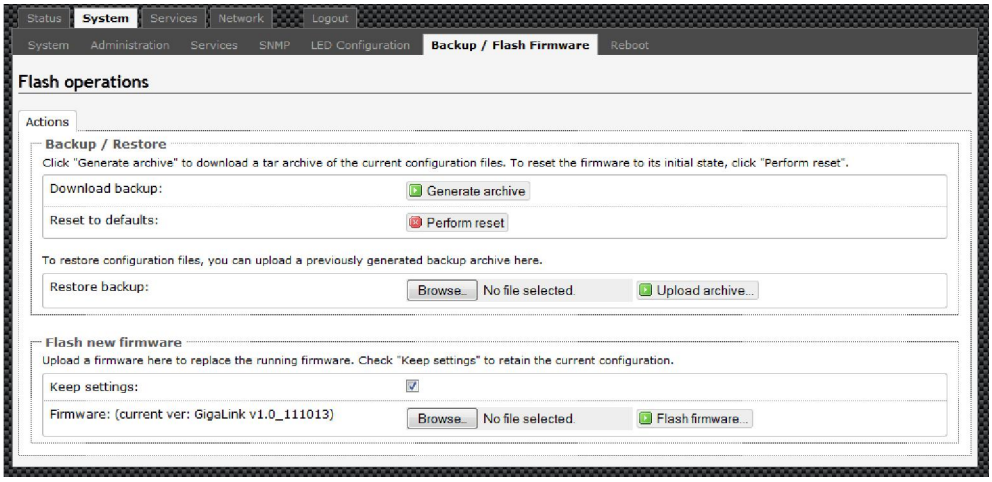




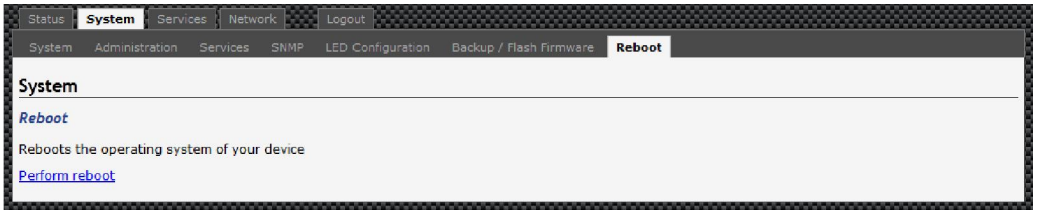
System - LED, let the user specify the Rx LEDs thresholds;



System - Backup/Flash Firmware, allows the user to do backup and save for the unit configuration, and upload new firmware versions.

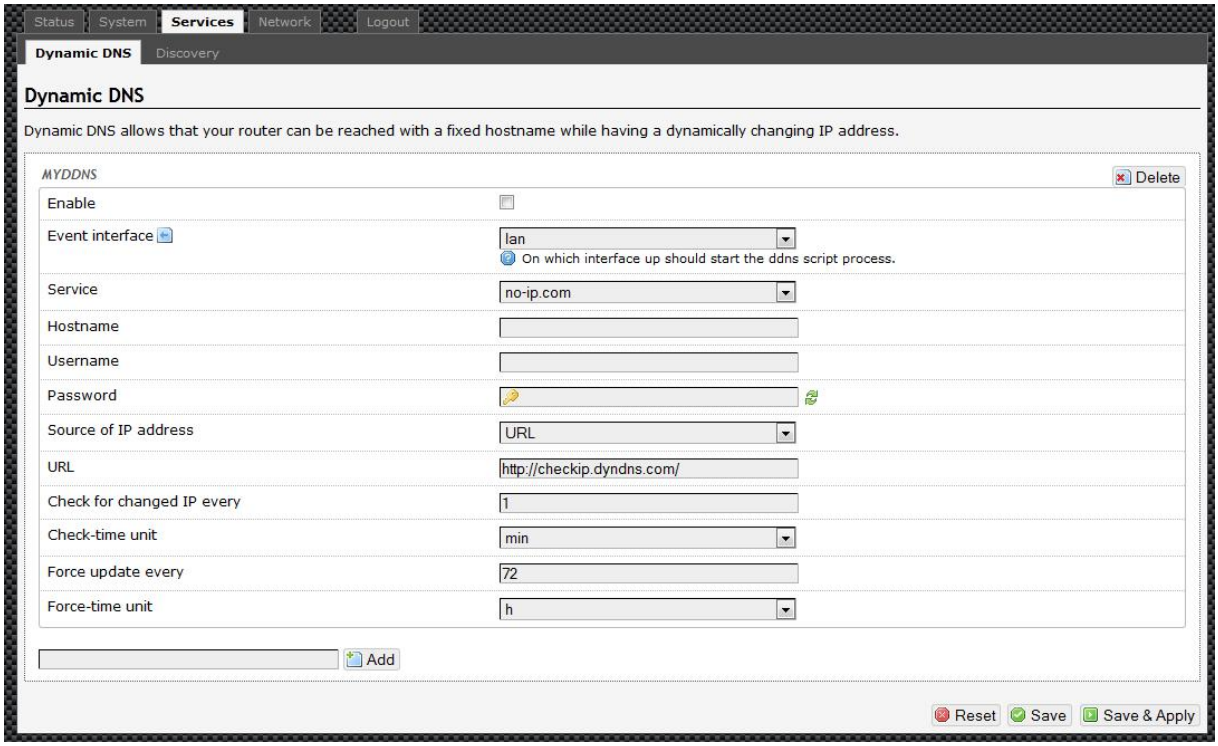


System - Reboot, allows the user to reboot the unit:

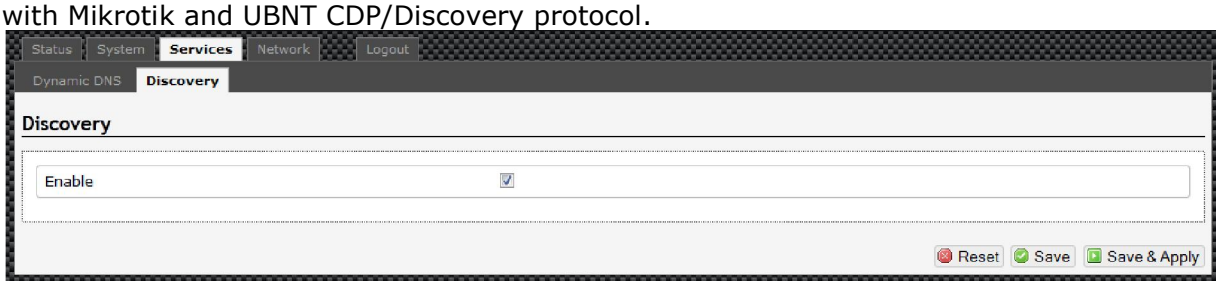


Services – Menu

Dynamic DNS, allows the user to specify a configuration to support Dynamic DNS:

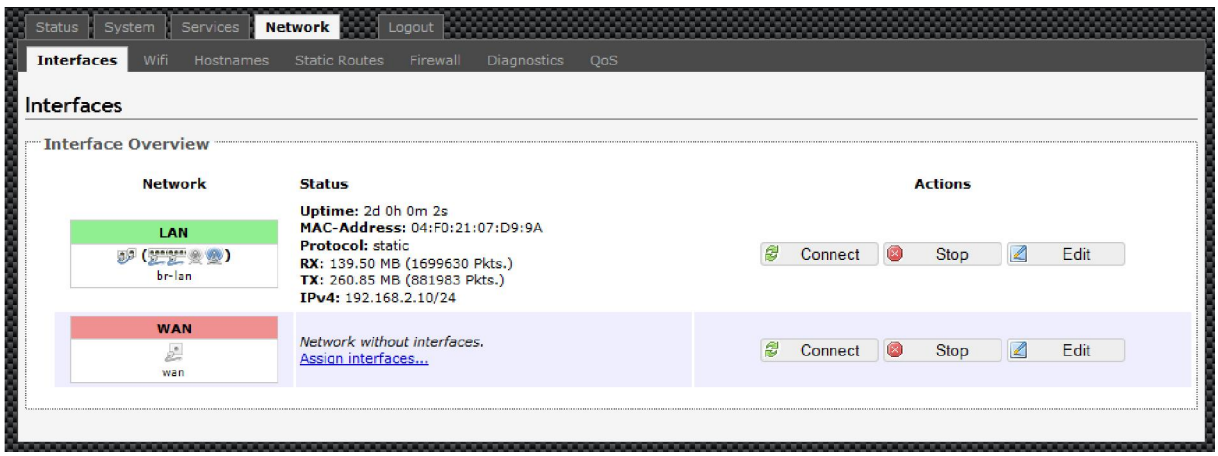


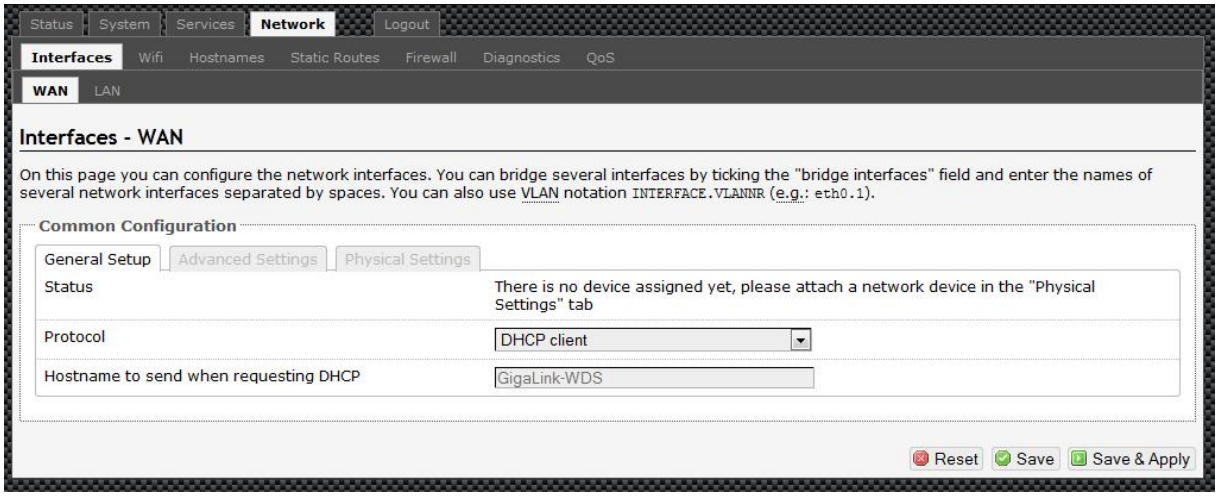
Discovery, enables/disables of CDP where the unit broadcasts it hostname. Compatible with Mikrotik and UBNT CDP/Discovery protocol.



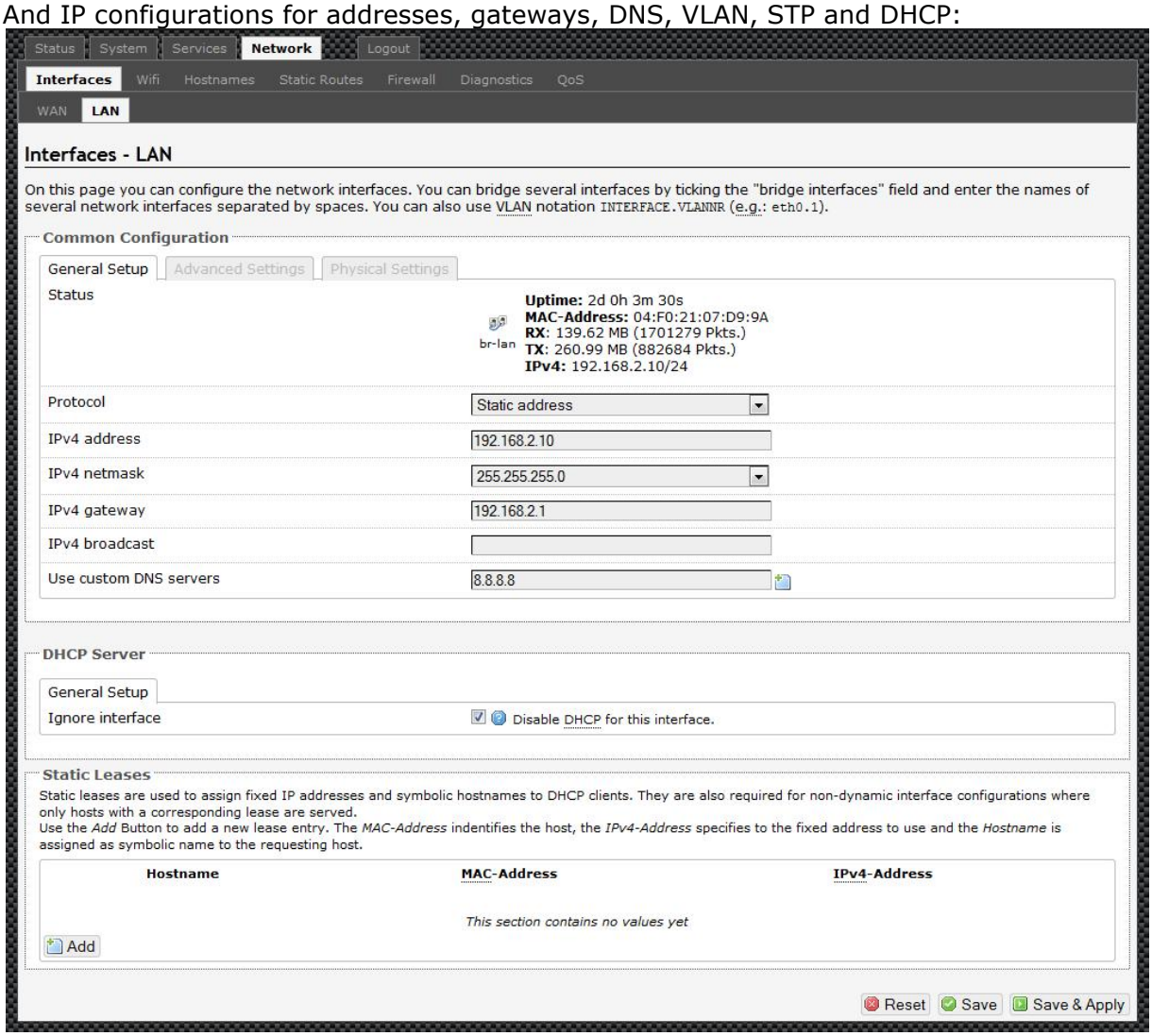
NETWORK - Menus

Network - Interfaces, allows user to specify configuration for LAN/WAN modes:

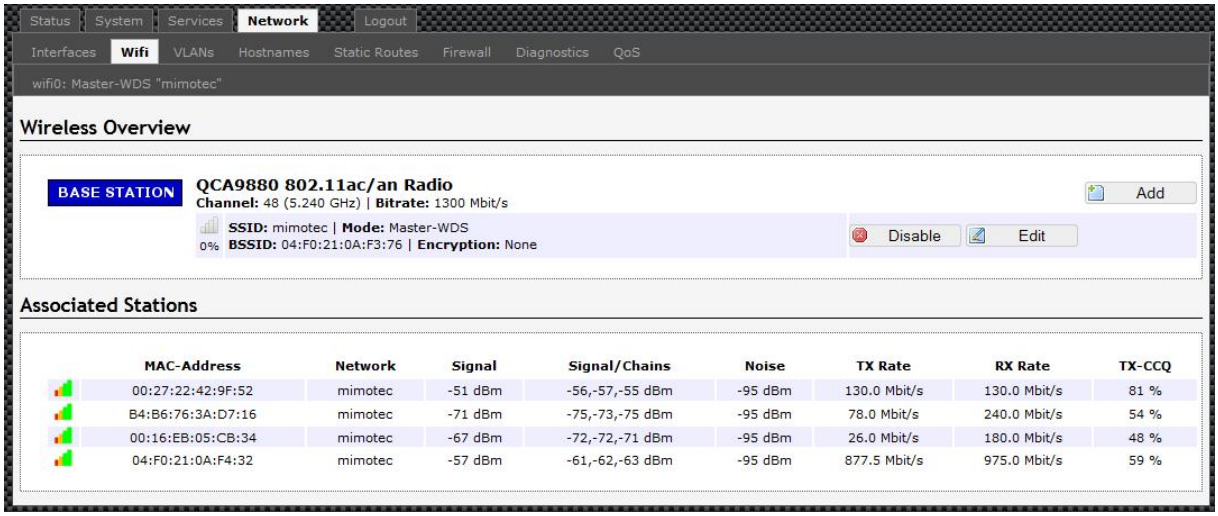


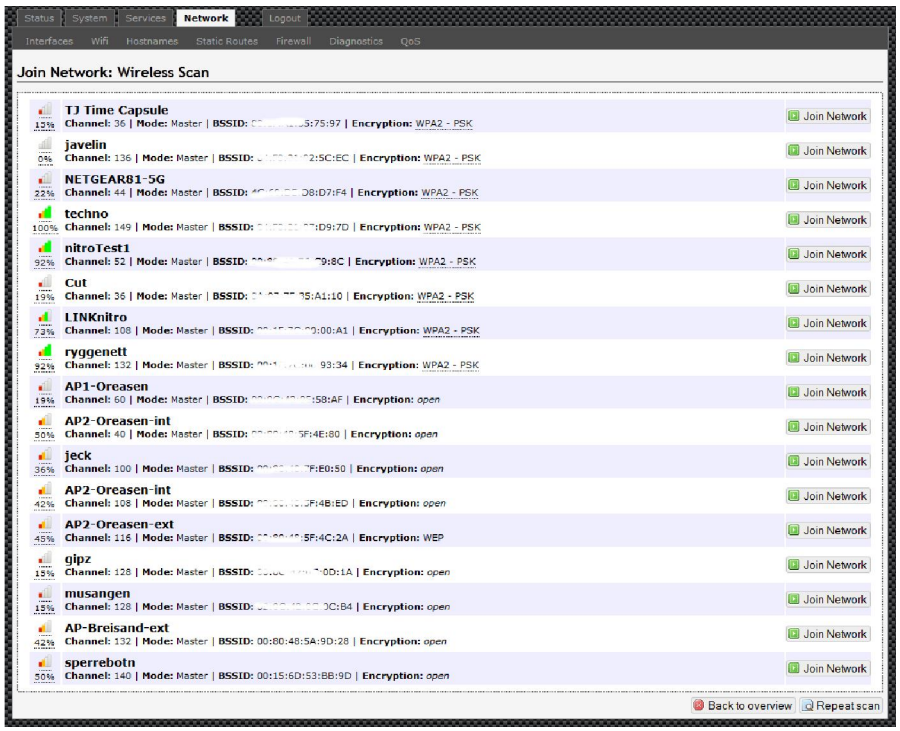


And IP configurations for addresses, gateways, DNS, VLAN, STP and DHCP:

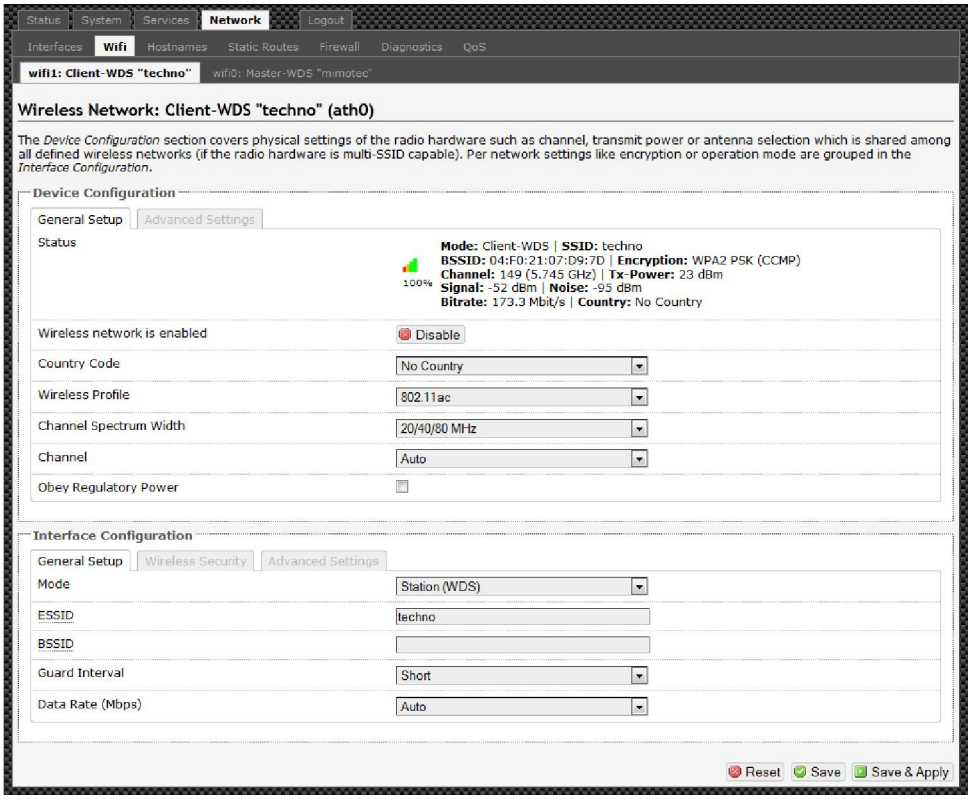


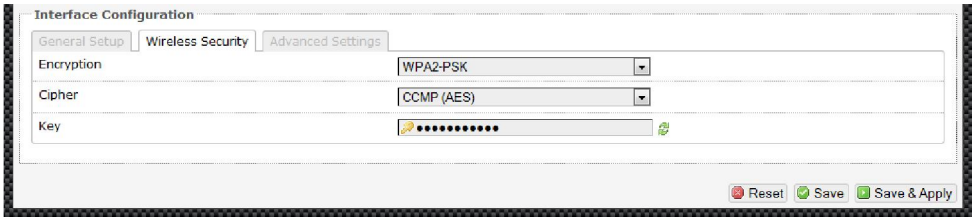
Network - WiFi, shows the user the running status of the wireless interfaces, and allows to edit and do RF-scans:



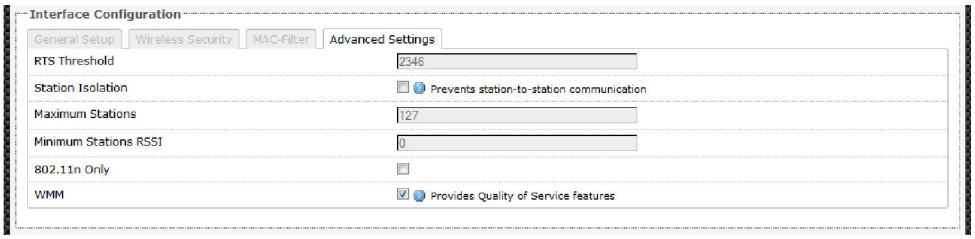

Status
System
Services
Network
Logout
Interfaces
Wifi
Hostnames
Static Routes
Firewall
Diagnostics
QoS
Join Network: Wireless Scan
TJ Time Capsule
Channel: 36 | Mode: Master | Encryption: WPA2 - PSK
javelin
Channel: 136 | Mode: Master | Encryption: WPA2 - PSK
NETGEAR81-5G
Channel: 44 | Mode: Master | Encryption: WPA2 - PSK
techno
Channel: 149 | Mode: Master | Encryption: WPA2 - PSK
nitroTest1
Channel: 52 | Mode: Master | Encryption: WPA2 - PSK
Cut
Channel: 36 | Mode: Master | Encryption: WPA2 - PSK
LINKnitro
Channel: 108 | Mode: Master | Encryption: WPA2 - PSK
ryggenett
Channel: 132 | Mode: Master | Encryption: WPA2 - PSK
AP1-Oreasen
Channel: 60 | Mode: Master | Encryption: open
AP2-Oreasen-int
Channel: 40 | Mode: Master | Encryption: open
jeck
Channel: 100 | Mode: Master | Encryption: open
AP2-Oreasen-int
Channel: 108 | Mode: Master | Encryption: open
AP2-Oreasen-ext
Channel: 116 | Mode: Master | Encryption: WEP
gjpz
Channel: 128 | Mode: Master | Encryption: open
musangen
Channel: 128 | Mode: Master | Encryption: open
AP-Breisand-ext
Channel: 132 | Mode: Master | BSSID: 00:80:48:5A:9D:28 | Encryption: open
sperrebotn
Channel: 140 | Mode: Master | BSSID: 00:15:6D:53:BB:9D | Encryption: open
Join Network
Back to overview
Repeat scan

WiFi - Edit Inteface, allows the user to set configuration parameters for the wireless interfaces:

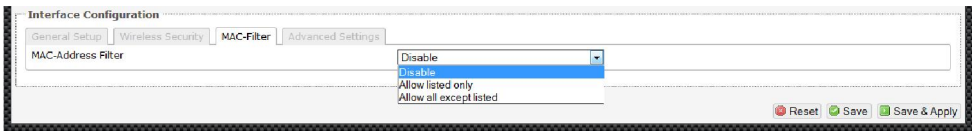

Status System Services Network Logout
Interfaces Wifi Hostnames Static Routes Firewall Diagnostics QoS
wifi1: Client-WDS "techno" wifi0: Master-WDS "mimotec"
Wireless Network: Client-WDS "techno" (ath0)
The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which is shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the Interface Configuration.
Device Configuration
General Setup Advanced Settings
Status
Mode: Client-WDS | SSID: techno
BSSID: 04:F0:21:07:D9:7D | Encryption: WPA2 PSK (CCMP)
Channel: 149 (5.745 GHz) | Tx-Power: 23 dBm
Signal: -52 dBm | Noise: -95 dBm
Bitrate: 173.3 Mbit/s | Country: No Country
Wireless network is enabled
Disable
Country Code
No Country
Wireless Profile
802.11ac
Channel Spectrum Width
20/40/80 MHz
Channel
Auto
Obey Regulatory Power
Interface Configuration
General Setup Wireless Security Advanced Settings
Mode
Station (WDS)
ESSID
techno
BSSID
Guard Interval
Short
Data Rate (Mbps)
Auto
Reset Save Save & Apply



If enabled, Station Isolation will prevent inter CPE communication.
It's possible to limit the number of CPE/Stations to connect to the Base Station
It's possible to avoid legacy stations to connect by selecting 802.11 Only
Priority for VWM (Wireless Multi Media) is supported if enabled.

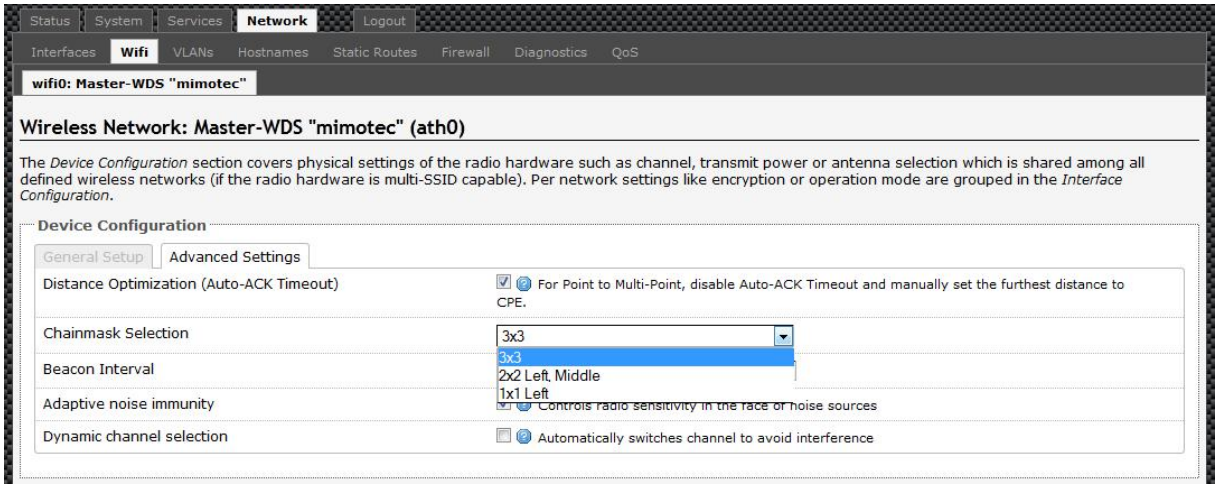


For Base Station mode, a ACL is available (MAC filter for allow/disallow) for stations.



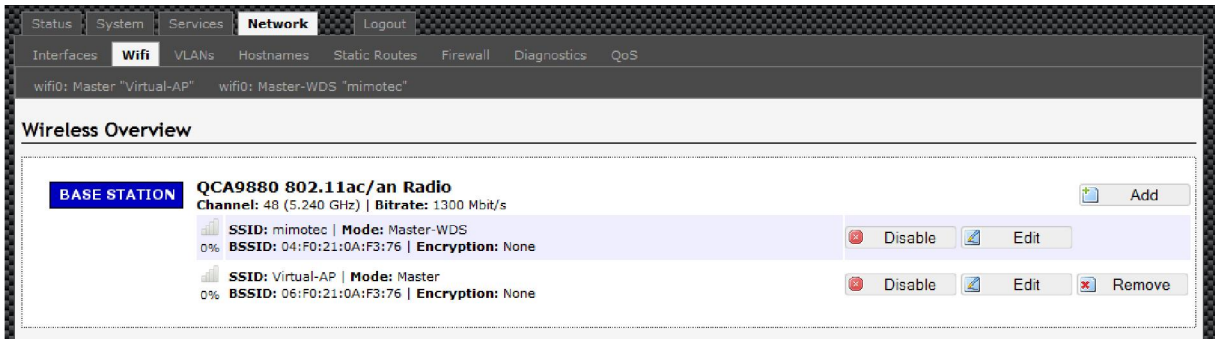
Device - Advanced Settings, allows user to select Auto or Manual Range, and to specify MIMO chains to be used - 1x1, 2x2 or 3x3 (if available). Select manual distance on Base Station if the unit is used in Point to Multi Point mode to avoid the renegotiations

of ack-time every time a CPE/Station connects/disconnects. In this case set the distance to the furthest CPE.

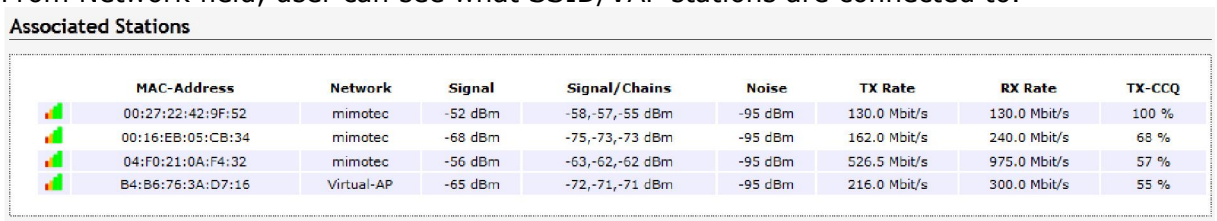


Adaptive noise immunity will if enabled, fine-tune the transceiver settings for optimal balance of TX power vs Receiver sensitivity related to noise levels detected.
Dynamic channel selection is supported, and if enabled the Base Station will move away from interfered channels if operation in automatic channel mode.

Virtual AP (VAP/Multi BSSID). User may create VAPs by selecting ADD in Network-WiFi menu. Set the wanted SSID and Security settings and apply settings.

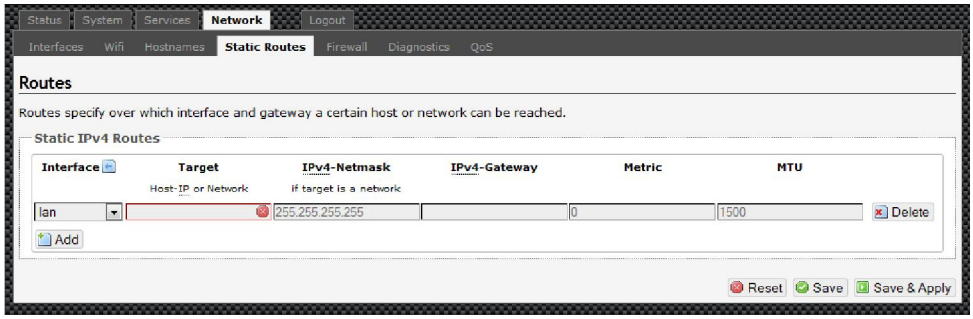


From Network field, user can see what SSID/VAP stations are connected to.

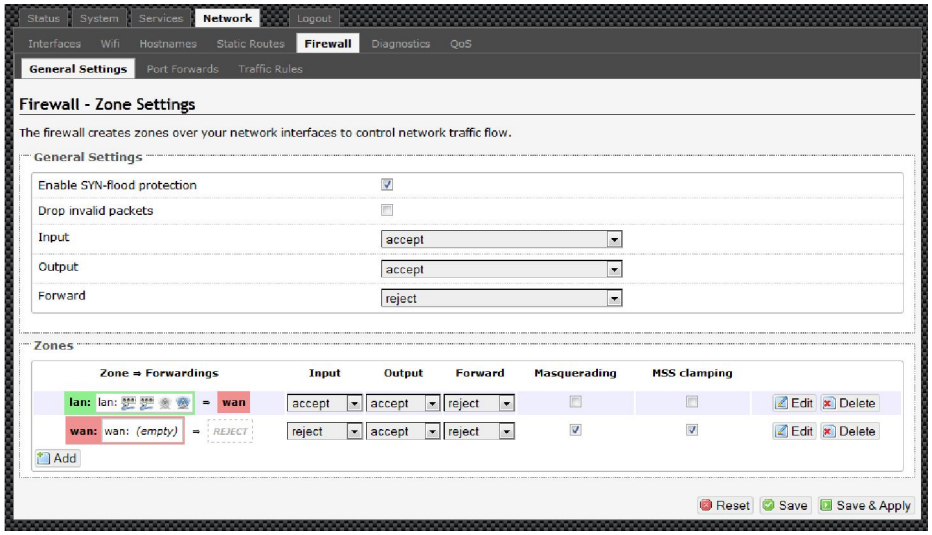


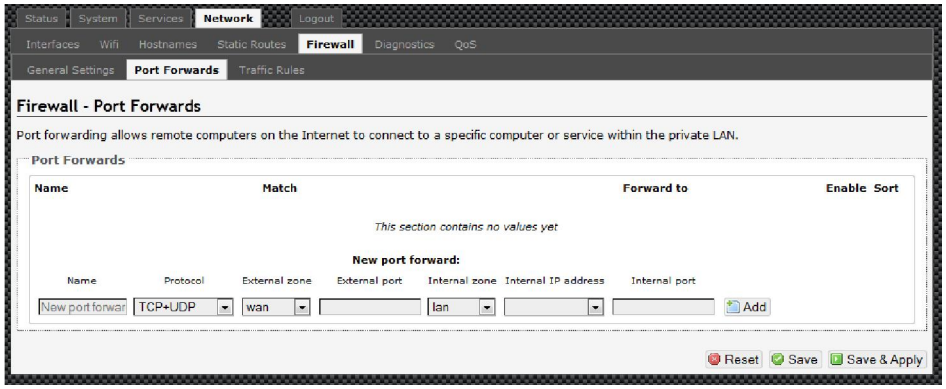
Network - Hostnames, allows user to specify network hosts by IP-addresses:

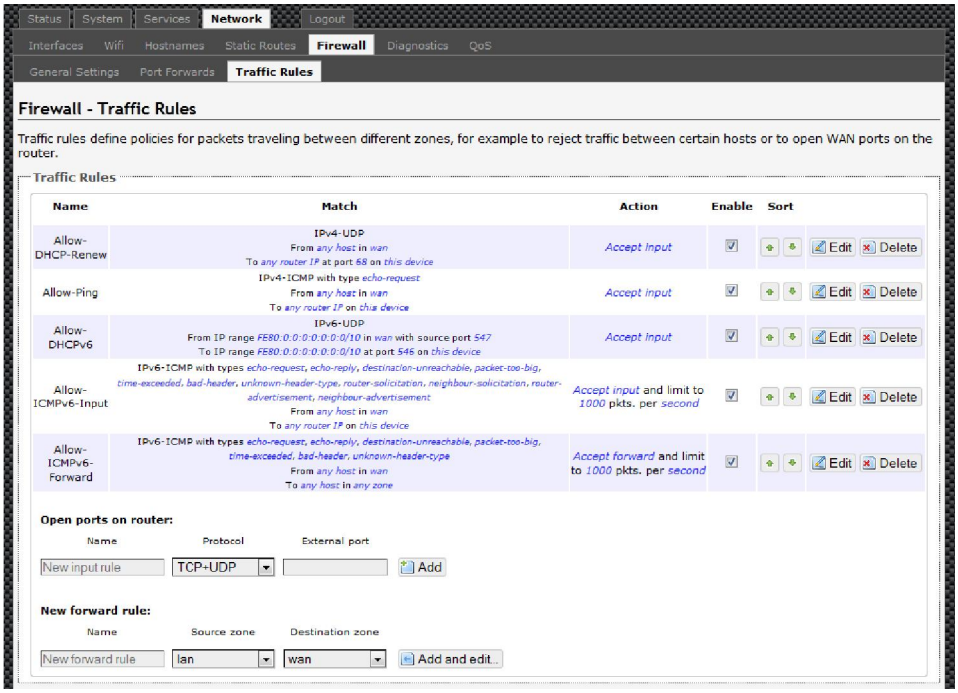
Network - Static Routes, allows user to specify routes and gateways for related networks:



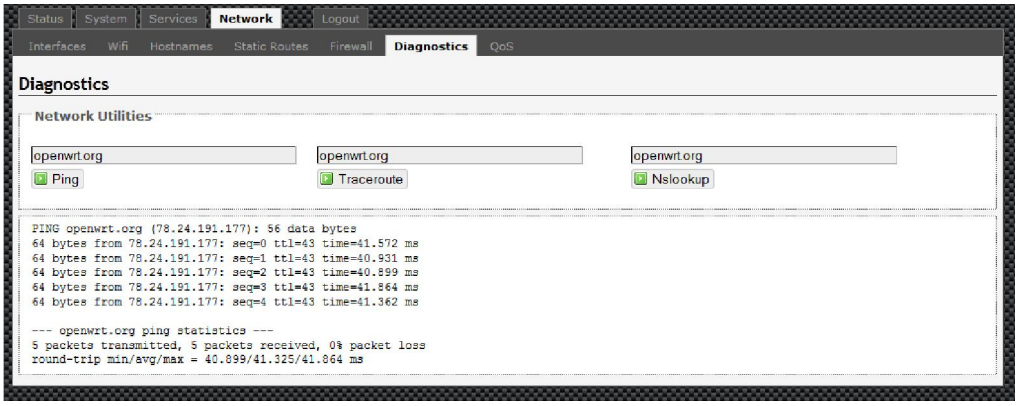
Network - Firewall, allows user to specify firewall rules by type and interface, and specify Port Forwarding and Traffic Rules:



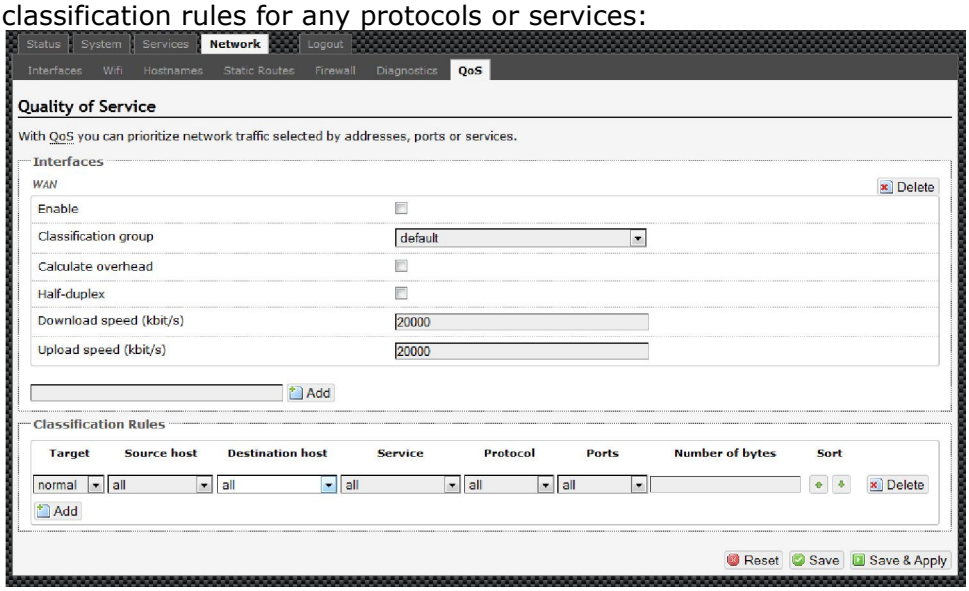



Status System Services Network Logout
Interfaces Wifi Hostnames Static Routes Firewall Diagnostics QoS
General Settings Port Forwards Traffic Rules
Firewall - Traffic Rules
Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.
Traffic Rules
Name Match Action Enable Sort
Allow-DHCP-Renew IPv4-UDP From any host in wan To any router IP at port 68 on this device Accept input Edit Delete
Allow-Ping IPv4-ICMP with type echo-request From any host in wan To any router IP on this device Accept input Edit Delete
Allow-DHCPv6 IPv6-UDP From IP range FE80:0:0:0:0:0:0:0/10 in wan with source port 547 To IP range FE80:0:0:0:0:0:0:0/10 at port 546 on this device Accept input Edit Delete
Allow-ICMPv6-Input IPv6-ICMP with types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-solicitation, router-advertisement, neighbour-advertisement From any host in wan To any router IP on this device Accept input and limit to 1000 pkts. per second Edit Delete
Allow-ICMPv6-Forward IPv6-ICMP with types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type From any host in wan To any host in any zone Accept forward and limit to 1000 pkts. per second Edit Delete
Open ports on router:
Name Protocol External port
New input rule TCP+UDP Add
New forward rule:
Name Source zone Destination zone
New forward rule lan wan Add and edit...

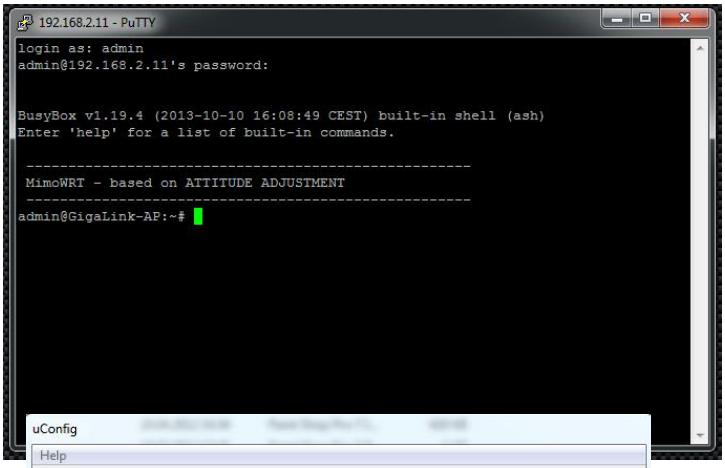
Network - Diagnostics, allows the user to verify network configuration with Ping, Traceroute and Nslookup:


Status System Services Network Logout
Interfaces Wifi Hostnames Static Routes Firewall Diagnostics QoS
Diagnostics
Network Utilities
openwrt.org Ping
openwrt.org Traceroute
openwrt.org Nslookup
PING openwrt.org (78.24.191.177): 56 data bytes
64 bytes from 78.24.191.177: seq=0 ttl=43 time=41.572 ms
64 bytes from 78.24.191.177: seq=1 ttl=43 time=40.931 ms
64 bytes from 78.24.191.177: seq=2 ttl=43 time=40.899 ms
64 bytes from 78.24.191.177: seq=3 ttl=43 time=41.864 ms
64 bytes from 78.24.191.177: seq=4 ttl=43 time=41.362 ms
--- openwrt.org ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 40.899/41.325/41.864 ms

Network - QoS, allows user to specify QoS rules pr type and interface, and create classification rules for any protocols or services:

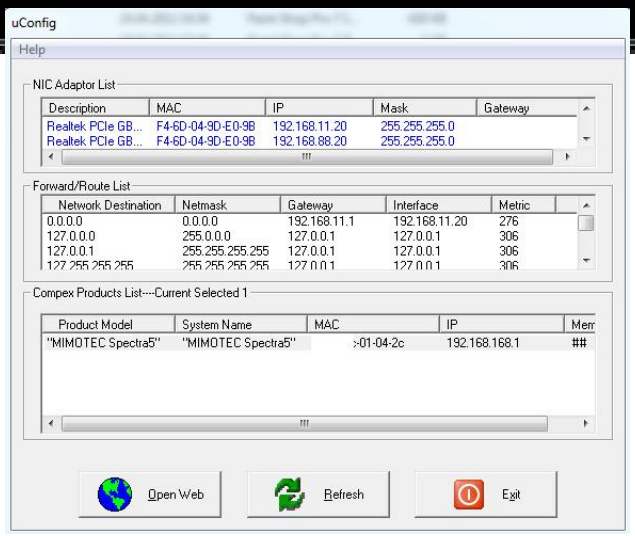

Status System Services Network Logout
Interfaces Wifi Hostnames Static Routes Firewall Diagnostics QoS
Quality of Service
With QoS you can prioritize network traffic selected by addresses, ports or services.
Interfaces
WAN Delete
Enable
Classification group default
Calculate overhead
Half-duplex
Download speed (kbit/s) 20000
Upload speed (kbit/s) 20000
Add
Classification Rules
Target Source host Destination host Service Protocol Ports Number of bytes Sort
normal all all all all all Delete
Add
Reset Save Save & Apply

External - Configuration


192.168.2.11 - PuTTY
login as: admin
admin@192.168.2.11's password:
BusyBox v1.19.4 (2013-10-10 16:08:49 CEST) built-in shell (ash)
Enter 'help' for a list of built-in commands.
MimoWRT - based on ATTITUDE ADJUSTMENT
admin@GigaLink-AP:~#

The SSH gives the admin access to Linux/BusyBox shell (Linux shell).

A balanced set of Linux tools and utilities are included, but Linux commands are not scope of this User Manual. Use with cautions.



Software Tools: All Spectra/Velocity/GigaLink units supports a Windows program that can be used to detect any active units on Layer2 (Mac Layer) for management.

uConfig is compatible with most MS Windows versions – including Vista and Windows 7 & 8.

Note: If Open Web is selected, the uConfig will temporarily implement a ipconfig setting compatible with unit IP-address.

Resetting the configuration:
If you need to reset the config to default settings without access to web-interface, you may use the standard OpenWRT prosedure via Telnet/SSH commands:

- firstboot
- reboot -f

Resetting the configuration by Reset Button:
You may reset the unit configuration back to default settings by holding the reset button pressed for 5 seconds or more (less than 30 sec). If the button is pressed for less than 5 seconds the unit will just do a reboot, and if held for more than 30 seconds will cancel the reset command.

Best Practice

By design, wireless systems are bridged/hub'ed technology. It's recommended to design your network based on bridging to get maximum performance, and rather do network segmentation than implement routing to achieve scalability. In any bridge mode (BTS or PtP), the WAN interface should be disabled or not connected to any interface.

Point To Point Links:

- Enable as few services as possible, to allow the CPU have all resources available for traffic handling
- Make sure the MIMO chains are balanced as equal as possible to each other.
- When all is aligned, consider setting a fixed range to prevent any later range drifting issues.

Base Station:

- Enable as few services as possible, to allow the CPU have all resources available for traffic handling
- When all is installed and aligned, set a fixed maximum range to prevent any later range calculation issues in connect/disconnect situations. Set the range to the maximum to be covered by the Base Station - the distance to the furthest station.
- Long range coverage will limit capacity of the Base Station - it's recommended to limit to maximum 4-6 km coverage on a 60-90 degree Base Station.